1.7 "**Bound Recording Method**" shall mean a method for recording content that effectively and uniquely associates such content with a single Licensed Product (using a cryptographic protocol or other effective means) so that the content of such recording cannot be accessed in usable form by another product except where such content is passed to or accessed by such product via a method permitted under these Compliance Rules.

1.8 "**Bound Recording**" shall mean a recording made using a Bound Recording Method.

1.9 "**Broadcast Flag**" shall mean (i) for unencrypted digital terrestrial broadcast television transmissions ("DTV Content") originating in the United States and its territories under the jurisdiction of the Federal Communications Commission, the Redistribution Control descriptor (rc_descriptor()) described in ATSC Standard A/65B: "Program and System Information Protocol for Terrestrial Broadcast and Cable." and (ii) for unencrypted digital terrestrial broadcast television transmissions originating in any other jurisdiction in which a similar law or regulation requires consumer electronics products and Computer Products to respond to a flag or trigger associated with such transmissions so as to restrict unauthorized redistribution thereof, such flag or trigger so identified in such law or regulation.

1.10 "**CGMS-A**" shall mean the Copy Generation Management System (analog) as specified (a) for 525/60 interlace scan analog video systems, in IEC 61880 (for inclusion of such value on line 20) or EIA-608-B (for inclusion of such value in line 21), (b) for 625/50 interlace scan analog video systems in ETS 300294 (for inclusion of such value on line 23), (c) for 525/60 progressive scan analog video systems, in IEC61880-2 (for inclusion on line 41), (d) for 625/50 progressive scan analog video systems, in IEC62375 (for inclusion on line 43), and (e) for 750/60 progressive or 1125/60 interlace scan analog video systems, in EIAJCPR 1204-2 (defining the signal waveform carrying CGMS-A) and IEC61880 (defining the bit assignment for CGMS-A).

1.11 "**CGMS-D**" shall mean the Copy Generation Management System (Digital) as specified for the DV Format in the "Blue Book: Specifications of Consumer Use Digital VCRs (DV)".

1.12 "**Colorstripe**" shall mean the so-named copy control system specified for NTSC analog composite video signals in the document entitled "Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999".

1.13 "**Commercial Audiovisual Content**" shall mean any audio, video or audiovisual works that are (a) not created by a consumer; (b) offered for transmission, delivery or distribution, either generally or on demand, to subscribers or purchasers or the public at large, or otherwise for commercial purposes, not uniquely to an individual, or a small or private group; and (c) encoded with Content Control Information.

1.14 "**Computer Product**" shall mean a device that is designed for or permits the end user to install a variety of commercially available software applications thereon, including but not limited to personal computers, handheld "Personal Digital Assistants," and the like and further includes a subsystem of such a device, such as a graphics card.

1.15 "**Constrained Image**" shall mean an image having the visual equivalent of no more than 520,000 pixels per frame (e.g. an image with resolution of 960 pixels by 540 pixels for a 16:9 aspect ratio). A Constrained Image may be attained by reducing resolution, for example, by discarding, dithering, or averaging pixels to obtain the specified value. A Constrained Image can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image. By way of example, a Constrained Image may be stretched or doubled, and displayed full-screen, on a 1000-line monitor.

1.16 "**Content Control Information**" shall mean the information that represents the content control status of particular content to a Licensed Product, including but not limited to Copy Control Information, APS Trigger Bits, EPN and ICT.

1.17 "**Copy Control Information**" shall mean the information that represents the copy control status of particular content to a Licensed Product, including but not limited to AGC, Colorstripe, CGMS-A, CGMS-D and, if Licensor has declared the Watermark, any information that represents copy control status that may be carried in the Watermark.

1.18 "**Copy Control Not Asserted**" refers to audiovisual content for which limitations on copying are not asserted. For the purpose of clarification and avoidance of doubt, such audiovisual content remains subject to the rights of the copyright owner. For further clarification and avoidance of doubt, audiovisual data that is not labeled with Content Control Information, is treated as Copy Control Information status is Copy Control Not Asserted.

1.19 "**Copy Never**" refers to Commercial Audiovisual Content that has been labeled as Copy Never indicating that no copies are to be made of such content.

1.20 "**Copy One Generation**" refers to Commercial Audiovisual Content that has been labeled as Copy One Generation indicating that only one generation of copies is to be made of such content.

1.21 "**Decrypted SVR Data**" shall mean, with respect to a Licensed Product, SVR Data that has been decrypted by such Licensed Product in accordance with the SVR CP Specifications and has not been re-encrypted using MG-R(SVR).

1.22 "**DTCP**" shall mean Digital Transmission Content Protection, a certain method for encryption, decryption, key exchange, authentication and renewability licensed by Digital Transmission Licensing Administrator, LLC for purposes of protecting certain digital content from unauthorized interception and copying.

1.23 "**DV Format**" shall mean the format defined in the specifications set by HD Digital VCR Conference for standardization of consumer use digital video formats.

1.24 "**EPN**" shall mean an encoding method, including but not limited to the Broadcast Flag, that indicates that Commercial Audiovisual Content is to be protected against unauthorized redistribution and that copy control restrictions are not being asserted with respect to such content.

1.25 "**EPN Asserted**" shall mean that EPN is asserted.

1.26 "**EPN Unasserted**" shall mean that EPN is not asserted. For clarification and avoidance of doubt, audiovisual content received via an Authorized Access Control Method for which an EPN trigger is not present, or via terrestrial digital television broadcast for which the Broadcast Flag is not present, shall be deemed to be labeled EPN Unasserted.

1.27 "**HDCP**" shall mean High-bandwidth Digital Content Protection, a certain method for encryption, decryption, key exchange, authentication and renewability licensed by the Digital Content Protection, LLC for purposes of protecting certain digital content from unauthorized interception and copying.

1.28 "**HDD**" shall mean a hard disk drive.

1.29 "**High Definition Analog Form**" shall mean a format that is an analog video signal that has a resolution greater than a Constrained Image.

1.30 "**High Definition Analog Output**" shall mean an analog output capable of transmitting Commercial Audiovisual Content in High Definition Analog Form.

1.31 "**Image Constraint Token**" or "**ICT**" shall mean the field or bits, as described in the SVR CP Specifications, used to trigger the output of a Constrained Image in Licensed Products.

1.32 "**Licensed Product**" shall mean a product that (i) embodies the designs set out in the SVR CP Specifications and (ii) is in compliance with all applicable portions of the SVR CP Specifications, Compliance Rules and Robustness Rules.

1.33 "**Logically Bound Copies**" shall have the meaning given in Section 2.4.

1.34 "**Memory Stick PRO Media**" shall mean IC recording media that conforms to applicable specifications for Memory Stick PRO specified by Licensor.

1.35 "**Memory Stick PRO Recording Function**" shall mean the function of a Licensed Product capable of recording, or causing to be recorded, Commercial Audiovisual Content on Memory Stick PRO Media in accordance with the SVR CP Specifications.

1.36 "**Move**" shall mean, with respect to Commercial Audiovisual Content, moving from media containing such content protected with MG-R(SVR) or from an HDD to a recording function using MG-R(SVR) or to an HDD recording function pursuant to Sections 4.2 ,4.3, 4.4(a).

1.37 "**No More Copies**" refers to Commercial Audiovisual Content that has been labeled No More Copies, indicating that it may have originated as Copy One Generation, but that the version being transmitted is from that first generation copy and that therefore no more copies are permitted.

1.38 "**Presently Known Watermark Technologies**" shall mean the technology submitted by VWM Companies to the DVD Copy Control Association, Inc. in November 2001 and the technology defined as ARIS/SOLANA-4C, as required by the SDMI Portable Device Specifications, Part 1, Version 1.0 (July 8, 1999).

1.39 "**Standard Definition Analog Output**" shall mean an analog output not capable of transmitting Commercial Audiovisual Content in High Definition Analog Form.

1.40 "**SVR Data**" shall mean, with respect to a Licensed Product, content that is encrypted using MG-R(SVR), or was previously encrypted by such Licensed Product using MG-R(SVR), but in each case has not been (a) passed to an output permitted by these Compliance Rules or (b) protected by recording technology other than MG-R(SVR) that constitutes an Authorized Access Control Method and is permitted under Section 4.5(i). For avoidance of doubt, SVR Data includes Decrypted SVR Data.

1.41 "**Thumbnail Copy**" shall have the meaning given in Section 2.4.

1.42 "**Watermark**" shall mean the watermark technology that will be designated as the Watermark for MG-R(SVR) by Licensor in its sole discretion.

1.43 "**YUV**" shall mean a component video output comprised of a luminance signal (Y) and two color difference signals (U and V) and specifically includes the following component video signals (Y, Pb, Pr), (Y, Cb, Cr), (Y, Db, Dr) and (Y, B-Y, R-Y).

2. Recording Control for Licensed Products that have a Memory Stick PRO Recording Function

2.1 Rules for Inputs Protected by Authorized Protection Methods

The Compliance Rules specified in this Section 2.1 are applicable solely to Licensed Products with respect to the recording by their Memory Stick PRO Recording Functions onto Memory Stick PRO Media of Commercial Audiovisual Content received through an Authorized Protection Method, provided that, except as expressly provided in Section 4, this Section 2.1 shall not apply with respect to recordings made pursuant to Section 4.

2.1.1 Copy Never

Licensed Products shall not make, or cause to be made, a copy on Memory Stick PRO Media of Commercial Audiovisual Content labeled "Copy Never."

2.1.2 No More Copies

Licensed Products shall not make, or cause to be made, a copy on Memory Stick PRO Media of Commercial Audiovisual Content labeled "No More Copies." For avoidance of doubt, nothing in this Section 2.1.2 shall restrict a Licensed Product from making Thumbnail Copies on, or Moving content to, Memory Stick PRO Media pursuant to Sections 2.4, 4.3 or 4.4(a).

2.1.3 Permitted Copy One Generation Copies

Licensed Products shall not make, or cause to be made, copies on Memory Stick PRO Media of Commercial Audiovisual Content labeled "Copy One Generation" unless such copies are encrypted using MG-R(SVR) and the Copy Control Information is updated according to the SVR CP Specifications to reflect the fact that a copy is being made.

2.1.4 EPN Encoded Content

Licensed Products may make, or cause to be made, a copy on Memory Stick PRO Media of Commercial Audiovisual Content labeled "EPN Asserted" only if each copy is encrypted by using MG-R(SVR). In such case, no updating of Copy Control Information is required.

2.2 Rules for Other Digital Inputs of Licensed Products

The Compliance Rules specified in this Section 2.2 are applicable solely to Licensed Products with respect to the recording by their Memory Stick PRO Recording Functions onto Memory Stick PRO Media of Commercial Audiovisual Content received through digital inputs, other than Authorized Protection Methods, provided that, except as expressly provided in Section 4, this Section 2.2 shall not apply with respect to recordings made pursuant to Section 4.

2.2.1 Digital Inputs other than Inputs through Authorized Protection Methods—General

For avoidance of doubt, no restrictions shall apply to recordings made from audiovisual content received by a Licensed Product via digital inputs other than Authorized Protection Methods, except as expressly set forth in Section 2.2.2.

2.2.2 Digital Signal Inputs in the DV Format

2.2.2.1 Licensed Products shall scan for CGMS-D associated with Commercial Audiovisual Content received in the DV Format prior to making such a recording of such content on Memory Stick PRO Media. Licensed Products shall be constructed such that, if CGMS-D is detected in such content, the following terms shall apply:

(a) Licensed Products shall not make, or cause to be made, a copy on Memory Stick PRO Media of Commercial Audiovisual Content labeled "Copy Never."

(b) Licensed Products shall not make, or cause to be made, a copy on Memory Stick PRO Media of Commercial Audiovisual Content labeled "Copy One Generation" unless such copy is encrypted using MG-R(SVR) and the Copy Control Information is updated according to the SVR CP Specifications to reflect the fact that a copy is being made.

2.2.2.2 Licensee is advised that Licensor anticipates amending these Compliance Rules in accordance with ARTICLE III of the Content Protection License Agreement to require detection of Content Control Information (e.g. CGMS-D) in other digital formats when Content Control Information is standardized for such other formats.

2.3 Rules for Analog Inputs of Licensed Products

The Compliance Rules specified in this Section 2.3 are applicable solely to Licensed Products with respect to the recording by their Memory Stick PRO Recording Functions onto Memory Stick PRO Media of Commercial Audiovisual Content received through analog inputs provided that, except as expressly provided in Section 4, this Section 2.3 shall not apply with respect to recordings made pursuant to Section 4.

Licensed Products shall not make, or cause to be made, a copy on Memory Stick PRO Media signals received via an analog input, except for the following analog formats (i.e., analog formats for which AGC or CGMS-A have been standardized)

A. NTSC, PAL, or SECAM analog composite video signals including S-video in Y/C format, including the RF signal.

B. YUV analog component video signals.

C. RGB signals contained in a SCART connector that is carrying a PAL, SECAM or NTSC composite video signal, provided that the composite video signal is used for the synchronization reference for that RGB signal.

2.3.1 Licensed Products shall not make, or cause to be made, a copy on Memory Stick PRO Media of Commercial Audiovisual Content if Automatic Gain Control is encoded in the incoming analog signal.

2.3.2 If Commercial Audiovisual Content received via an analog input includes CGMS-A, CGMS-A shall be used to determine whether such Commercial Audiovisual Content may be recorded on Memory Stick PRO Media, and the following terms shall apply:

(a) such Licensed Product shall not make, or cause to be made, a copy on Memory Stick PRO Media of Commercial Audiovisual Content labeled "Copy Never."

(b) such Licensed Product shall not make, or cause to be made, a copy on Memory Stick PRO Media of Commercial Audiovisual Content labeled "Copy One Generation" unless such copy is encrypted using MG-R(SVR) and the Copy Control Information is updated according to the SVR CP Specifications to reflect the fact that a copy is being made.

2.4 Thumbnails

Notwithstanding any other provision of these Compliance Rules, in the event that a copy of Commercial Audiovisual Content has been recorded on a Memory Stick PRO Media or HDD with a label of "No More Copies" pursuant to Sections 2.1.3, 2.2.2.1(b), 2.3.2(b), 4.1, 4.2, 4.3 or 4.4(a) (any such "No More Copies" copy, an "Initial Copy"), such Licensed Product may make, or cause to be made, one or more generation copies on such Memory Stick PRO Media or HDD, as the case may be, of such Initial Copy (each, a "Thumbnail Copy"), only if (i) all Thumbnail Copies made directly or indirectly from such Initial Copy are stored on the same Memory Stick PRO Media or HDD, as the case may be; (ii) such Thumbnail Copies are encrypted using MG-R(SVR) (in the case of recordings on Memory Stick PRO Media) or are made using a Bound Recording Method (in the case of recordings on HDD); and (iii) such Thumbnail Copies are logically bound to such Initial Copy, such that if the Initial Copy or any of its Thumbnail Copies (collectively, such Initial Copies and Thumbnail Copies, "Logically Bound Copies") are later Moved from the Memory Stick PRO Media or HDD, none of its other Logically Bound Copies shall thereafter be accessed in useable form on such Memory Stick PRO Media or HDD.

2.5 Storage of Content Control Information

The Content Control Information detected and/or updated in accordance with Section 2.1.3, Section 2.2.2.1(b) or Section 2.3.2(b) at the time of recording shall be stored as described in SVR CP Specifications.

3. Output Controls

A Licensed Product shall be constructed such that it shall not pass, or direct to be passed, Decrypted SVR Data to an output, whether in digital or analog form, except as follows:

(a) Where the Decrypted SVR Data is output via an approved Standard Definition Analog Output pursuant to Section 3.1;

(b) Where the Decrypted SVR Data is output via a High Definition Analog Output pursuant to Section 3.2;

(c) Where the Decrypted SVR Data is output via a digital output pursuant to Section 3.3;

(d) Where the Decrypted SVR Data is labeled as "Copy Control Not Asserted" and "EPN Unasserted" in which case there are no restrictions on output; or

(e) in the case of the audio portion of Decrypted SVR Data, via any analog output.

3.1 Standard Definition Analog Outputs

A Licensed Product shall not pass, or direct to be passed, Decrypted SVR Data to an NTSC, YUV, SECAM, PAL or consumer RGB format analog output (including an S-video output for the listed formats) unless (a) such Decrypted SVR Data is labeled as other than "No More Copies", "Copy Never" or "Copy One Generation" or (b) such Licensed Product is incorporated into a Computer Product and the output is either a VGA output or a similar output that was widely implemented as of May 1, 2001 that carries uncompressed video signals with a resolution less than or equal to a Constrained Image or (c) such Licensed Product generates copy control signals according to the information provided in such Decrypted SVR Data using the technologies set forth in Sections 3.1.1 through 3.1.4:

3.1.1 For NTSC (525/60i systems) interlace scan analog video signal outputs, the specifications for (i) the Automatic Gain Control and Colorstripe copy control systems and (ii) generation of CGMS-A, provided that all of such technologies must be utilized in order to meet this requirement.

3.1.2 For PAL, SECAM (625/50i systems) or YUV (525/60i or 625/50i systems) interlace scan analog video signal outputs, the appropriate specifications for (i) the Automatic Gain Control copy control system and (ii) generation of CGMS-A, provided that both of these technologies must be utilized in order to meet this requirement.

3.1.3 For YUV (525/60p or 625/50p systems) progressive scan analog video signal outputs, the appropriate specifications for (i) the Automatic Gain Control copy control system and (ii) generation of CGMS-A, provided that all of such technologies must be utilized in order to meet this requirement.

3.1.4 For SCART connectors, the Automatic Gain Control specifications for the PAL, SECAM or NTSC signal carried by that connector, provided that the connector must be configured so that the component signal carried by the connector must always be accompanied by a composite signal and such composite signal must provide the only synchronization reference for the component signal.

3.1.5 Licensed Products shall apply Analog Protection System (APS) to Decrypted SVR Data labeled as "No More Copies" in accordance with the corresponding APS Trigger Bits identified in the SVR CP Specifications.

3.2 High Definition Analog Outputs

3.2.1 Licensed Products shall not pass, or direct to be passed, Decrypted SVR Data to a High Definition Analog Output, unless both requirements set forth in (i) and (ii) are fulfilled:

> **(i)** Such Licensed Products may pass, or direct to be passed, such Decrypted SVR Data to a High Definition Analog Output as a Constrained Image.
>
> **(ii)** Such Licensed Products may pass, or direct to be passed, Decrypted SVR Data to a High Definition Analog Output, if they generate copy control signals using CGMS-A, in accordance with the information provided in such Decrypted SVR Data.

3.2.2 Notwithstanding Section 3.2.1 above, such Licensed Products incorporated into Computer Products may pass, or direct to be passed, Decrypted SVR Data to XGA, SXGA and UXGA or similar computer video outputs that were widely implemented as of May 1, 2001 (but not to such typical consumer electronics outputs as NTSC, PAL, SECAM, SCART, YUV, S-Video and consumer RGB, whether or not such outputs are found on any Computer Product) as a Constrained Image.

3.3 Digital Outputs

3.3.1 Licensed Products may not pass, or direct to be passed, Decrypted SVR Data to a digital output except as follows:

(i) To DTCP protected outputs, provided that the Licensed Product shall pass, or direct to be passed, all appropriate Content Control Information associated with such content identified in the SVR CP Specifications to the DTCP Source Function so as to accurately set the DTCP Descriptor in accordance with the specification and license agreement for DTCP;

(ii) To HDCP protected outputs, provided that the Licensed Product shall confirm from the information provided by the HDCP Source Function that such HDCP Source Function is fully engaged and able to deliver Decrypted SVR Data in protected form in accordance with the specification and license agreement for HDCP;

(iii) In the case of Licensed Products incorporated into Computer Products, as a Constrained Image to DVI outputs of devices manufactured on or prior to June 30, 2005, unless otherwise notified by Licensor;

(iv) To any digital output where the Decrypted SVR Data is labeled "Copy Control Not Asserted" and also "EPN Unasserted"; or

(v) Via any other methods approved by Licensor.

3.3.2 Except as otherwise provided in Section 3.3.1 above, Licensed Products shall not output the audio portions of Decrypted SVR Data in digital form unless in compressed audio format (such as AC3) or in Linear PCM format in which the transmitted information is sampled at no more than 48kHz and no more than 16 bits.

4. Integrated Products

In the event that a Licensed Product includes (a) a Memory Stick PRO Recording Function or function capable of accessing in usable form content stored on a Memory Stick PRO Media and (b) functions capable of recording onto, or accessing in usable form content stored on, another storage medium, including but not limited to an HDD (such Licensed Product, an "Integrated Product"), the requirements of this Section 4 shall apply to such Licensed Product.

4.1 Recording Control for HDD Recordings By Integrated Products

In the event that there is a possibility that content recorded on an HDD by or at the direction of an Integrated Product may later be copied from such HDD to Memory Stick PRO Media by or at the direction of such Integrated Product, such Integrated Product shall not record on such HDD content received through digital inputs other than those protected by an Authorized Protection Method, or through an analog input, unless such Integrated Product records such content on such HDD in a manner pursuant to Section 2, provided that in lieu of any obligation to record content on a Memory Stick PRO Media by using MG-R(SVR), such Integrated Product shall make such recording using a

Bound Recording Method on the HDD. Recordings made on HDD from content received via an Authorized Access Control Method shall be subject to any restrictions imposed by the license for such Authorized Access Control Method.

4.2 Rules for Transmission Via Internal Connections From Memory Stick PRO Media to HDD

An Integrated Product shall not pass a copy of SVR Data recorded on Memory Stick PRO Media to an HDD recording function in or controlled by such Integrated Product unless (i) such SVR Data is labeled "Copy Control Not Asserted" or "EPN Asserted" or (ii) such SVR Data is labeled "No More Copies" and (a) such copy on Memory Stick PRO Media and all Thumbnail Copies made on the Memory Stick PRO Media directly or indirectly therefrom and any other Logically Bound Copies with respect thereto, are deleted from such Memory Stick PRO Media or otherwise rendered unusable and (b) such copy and any Logically Bound Copies with respect thereto that are also passed to such HDD recording function pursuant to this Section 4.2 remain Logically Bound Copies on such HDD. Except if such copy is labeled "Copy Control Not Asserted" and also "EPN Unasserted," such copy passed to an HDD recording function pursuant to this Section 4.2 must be stored on the HDD using a Bound Recording Method.

4.3 Rules for Transmission Via Internal Connections From HDD to Memory Stick PRO Recording Function

An Integrated Product shall not record or cause to be recorded onto Memory Stick PRO Media a copy passed to the Memory Stick PRO Recording Function of such Integrated Product of content stored on an HDD as a Bound Recording, where such HDD is contained in, or such Bound Recording is controlled by, the same Integrated Product unless (i) such content is labeled "Copy Control Not Asserted" or "EPN Asserted" or (ii) such content is labeled "No More Copies" and (a) such content on the HDD and all Thumbnail Copies made on such HDD directly or indirectly therefrom and any other Logically Bound Copies with respect thereto, are deleted from such HDD or otherwise rendered unusable and (b) such copy and any Logically Bound Copies with respect thereto that are also passed from such HDD to such Memory Stick PRO Recording Function pursuant to this Section 4.3 remain Logically Bound Copies on the Memory Stick PRO Media. Except if such copy is labeled "Copy Control Not Asserted" and also "EPN Unasserted," such copy must be encrypted on the Memory Stick PRO Media using MG-R(SVR).

4.4 Rules for Transmission Via Internal Connections From Storage Media Other Than HDD to Memory Stick PRO Recording Function

An Integrated Product shall not record or cause to be recorded onto Memory Stick PRO Media a copy passed to the Memory Stick PRO Recording Function of such Integrated Product of content stored on a storage medium, other than an HDD, where such storage medium is contained in, or content stored on such storage medium is controlled by, the same Integrated Product, unless:

(a) such content on such other storage medium is encrypted with MG-R(SVR) and (i) the content is labeled "Copy Control Not Asserted" or "EPN Asserted" or (ii) the content is labeled "No More Copies" and (x) such copy, and all Thumbnail Copies made on the same originating media directly or indirectly therefrom, and any other Logically Bound Copies with respect thereto, are deleted from the originating storage medium or otherwise rendered unusable; (y) such copy and any Logically Bound Copies with respect thereto that are also passed from such other storage medium to such Memory Stick PRO Recording Function pursuant to this Section 4.4 remain Logically Bound Copies on the destination Memory Stick PRO Media; and (z) such copy is encrypted on the destination Memory Stick PRO Media using MG-R(SVR);

(b) such content is passed from the other storage medium to the Memory Stick PRO Recording Function using an Authorized Access Control Method and such recording is not prohibited by the license applicable to such Authorized Access Control Method; or

(c) such recording can otherwise be made without violating any other applicable license agreement and in the event that any portion of a Program received through a digital input other than a digital input protected by an Authorized Protection Method, or through an analog input, is so passed to such Memory Stick PRO Recording Function from such other storage medium during the period during which such Program is being recorded on such other storage medium by or at the direction of such Integrated Product, such Integrated Product shall comply with the terms of Sections 2.2, 2.3 and 2.5 as if such Memory Stick PRO Recording Function received such Program directly from such digital or analog input. For purposes of this Section 4.4, "Program" shall mean any work of Commercial Audiovisual Content.

4.5 Rules for Transmission Via Internal Connections From Memory Stick PRO Media to Other Recording Functions

An Integrated Product shall not pass, or direct to be passed, SVR Data recorded on Memory Stick PRO Media to a recording function in or controlled by the same Integrated Product other than an HDD recording function (i) if the Copy Control Information is labeled "EPN Asserted" unless such recording is made using MG-R(SVR) or CPRM, D-VHS or any other recording method permitted under the applicable license for any output technology referenced in Section 3.3 or (ii) if the Copy Control Information is labeled "No More Copies" unless such SVR Data is passed to a recording function that uses MG-R(SVR).

4.6 Output Controls for HDD Content

For avoidance of doubt, the terms of Section 3 applicable to the output of Decrypted SVR Data shall apply with respect to the output of SVR Data stored on an HDD as a

Bound Recording.

5. Watermark

5.1 Watermark

Licensor may introduce mandatory screening requirements for a watermark technology in the future. Licensor hereby notifies and cautions Licensee, that these Compliance Rules may be modified in the future to ensure that these Compliance Rules are consistent with operation of the Watermark, including, but not limited to, recording control and playback control.

5.2 Watermark non-interference

During the period commencing on the Effective Date of the Content Protection License Agreement to which these Compliance Rules are attached and ending on the date Licensor designates the Watermark, Licensee shall not (a) knowingly design or knowingly develop Licensed Products or a component thereof for the primary purpose of stripping, obscuring, or changing the value of Presently Known Watermark Technologies in audiovisual content that is or may become SVR Data in such Licensed Products or such a component, or (b) knowingly promote, knowingly advertise or knowingly cooperate in the promotion or advertising of Licensed Products or a component thereof for the purpose of stripping, interfering or obscuring Presently Known Watermark in such audiovisual content.

5.3 Legitimate Product Features

Section 5.2 shall not prohibit a Licensed Product or a component thereof from incorporating legitimate features (i.e. zooming, scaling, cropping, picture-in-picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, down-sampling, up-sampling and line doubling or conversion between widely-used formats for the transport, processing and display of audiovisual signals or data, such as between analog and digital formats and between PAL and NTSC or RGB and YUV formats, as well as other features as may be added to the foregoing list from time to time by Licensor by amendment to these Compliance Rules) that are not prohibited by law, and such features shall not be deemed to strip, obscure, or change the value of Presently Known Watermark Technologies.

6. Hierarchy of labeling technologies

In the event that a conflict exists between or among multiple copy control labeling method, the following order of precedence shall control: (1) if Licensor has declared the Watermark, the Watermark; (2) AGC; (3) CGMS-A.

Exhibit D
Robustness Rules

1. Construction

1.1 Generally

Licensed Products, as shipped, shall meet the applicable Compliance Rules set forth in Exhibit C, and shall be manufactured in a manner clearly designed to effectively frustrate attempts to modify such Licensed Products to defeat the content protection requirements of MG-R(SVR) set forth in SVR CP Specifications and Compliance Rules.

1.2 Defeating Functions

Licensed Products shall not include:

(a) switches, buttons, jumpers or software equivalents thereof,

(b) specific traces that can be cut, or

(c) functions (including service menus and remote-control functions),

in each case by which the mandatory provisions of SVR CP Specifications or the Compliance Rules, including the content protection technologies, analog protections, output restrictions, recording protections or recording limitations can be defeated, or by which compressed Decrypted SVR Data in such Licensed Products can be exposed to output, interception, retransmission or copying, in each case other than as permitted under this Agreement.

1.3 Keep Secrets

Licensed Products shall be manufactured in a manner that is clearly designed to effectively frustrate attempts to discover or reveal Device Key Set, the Highly Confidential cryptographic algorithms used in MG-R(SVR), and any other Highly Confidential Information.

1.4 Robustness Checklist

Before releasing any Licensed Products, Licensee must perform tests and analyses to assure compliance with these Robustness Rules. A Robustness Checklist is attached as Exhibit D-1 for the purpose of assisting Licensee in performing tests covering certain important aspects of these Robustness Rules. Inasmuch as the Robustness Checklist does not address all elements required for the manufacture of a compliant product, Licensee is strongly advised to review carefully the SVR CP Specifications, Compliance Rules (including, for avoidance of doubt, these Robustness Rules) so as to evaluate thoroughly both its testing procedures and the compliance of its Licensed Products. Licensee shall provide copies of SVR CP Specifications, the Compliance Rules, these Robustness Rules and the Robustness Checklist to its supervisors responsible for design and manufacture of Licensed Products.

2. Data Paths

Decrypted SVR Data shall not be available on outputs other than those specified in the Compliance Rules. Within a Licensed Product, Decrypted SVR Data shall not be present on any user-accessible buses in analog or unencrypted, compressed form.

2.1 A "user accessible bus" means (a) an internal analog connector that: (i) is designed and incorporated for the purpose of permitting end user upgrades or access or (ii) otherwise readily facilitates end user access or (b) a data bus that is designed for end user upgrades or access, such as an implementation of a smartcard, PCMCIA, Cardbus, or PCI that has standard sockets or otherwise readily facilitates end user access. A "user accessible bus" *does not include memory buses, CPU buses, or similar portions of a device's internal* architecture that do not permit access to content in a form useable by end users.

Clause 2.1 (a) should be interpreted and applied so as to allow Licensee to design and manufacture its products to incorporate means, such as test points, used by Licensee or professionals to analyze or repair products; but not to provide a pretext for inducing consumers to obtain ready and unobstructed access to internal analog connectors. Without limiting the foregoing, with respect to Clause 2.1(a), an internal analog connector shall be presumed to not "ready facilitate end user access" if (i) such connector and the video signal formats or levels of signals provided to such connector, are of a type not generally compatible with the accessible connections on consumer products, (ii) such access would create a risk of product damage, or (iii) such access would result in physical evidence that such access has occurred and would void any product warranty.

2.2 Licensee is alerted that these Robustness Rules may be revised in the future, upon notification by Licensor, to require that, when Licensor deems that it is technically feasible and commercially reasonable to do so, Licensed Products be clearly designed such that when uncompressed, Decrypted SVR Data are transmitted over a User Accessible Bus, such Decrypted SVR Data are made reasonably secure from unauthorized interception by use of means that can be defeated neither by using Widely Available Tools nor by using Specialized Tools, except with difficulty, other than Circumvention Devices. The level of difficulty applicable to Widely Available Tools is such that a typical consumer should not be able to use Widely Available Tools, with or without instruction, to intercept such Decrypted SVR Data without risk of serious damage to the product or personal injury. Licensee is further alerted that, when it is deemed technically feasible and reasonably practicable to do so, Licensor will revise these Robustness Rules to require that uncompressed Decrypted SVR Data will be re-encrypted or otherwise protected before it is transmitted over such buses.

3. *Methods of Making Functions Robust.*

Licensed Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements set forth below.

3.1 Distributed Functions

In a Licensed Product, where SVR Data is delivered from one part of Licensed Product to another, whether among integrated circuits , software modules, or otherwise or a combination thereof, the portions of Licensed Products that perform authentication and/or decryption and the MPEG (or similar) decoder shall be designed and manufactured in a manner associated and otherwise integrated with each other such that Decrypted SVR Data in any usable form flowing between these portions of Licensed Products shall be reasonably secure from being intercepted or copied except as authorized by the Compliance Rules.

3.2 Software

Any portion of Licensed Products that implements any of the content portion requirements of SVR CP Specifications in Software shall include all of the characteristics set forth in Section 1 or 2 of Exhibit D. For the purpose of these Robustness Rules, "Software" shall mean the implementation of the content protection requirements as to which this agreement requires a Licensed Product to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations shall:

3.2.1 Comply with Section 1.3 of this Exhibit D by a reasonable method including, but not limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation; and, in addition, in every case of implementation in Software, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.

3.2.2 Be designed so as to perform self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized-authentication and/or decryption function. For the purpose of this provision, a "modification" includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections 1 and 2 of this Exhibit D. This provision requires at a minimum the use of "signed code" or more robust means of "tagging" operating throughout the code.

3.23 Hardware

Any portion of Licensed Products that implements any of the content protection requirements of SVR CP Specifications in Hardware shall include all of the characteristics set forth in Section 1 and 2 of this Exhibit D. For the purposes of these Robustness Rules, "Hardware" shall mean a physical devise, including a component, that implements any of the content protection requirements as to which this Agreement requires that a Licensed Product be compliant and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Licensed

Product and such instructions or data are not accessible to the end user through Licensed Product. Such implementations shall:

3.3.1 Comply with Section 1.3 of this Exhibit D by any reasonable method including, but not limited to, embedding Device Key Set and Highly Confidential cryptographic algorithms in silicon circuitry that cannot reasonably be read, or employing the techniques described above for Software.

3.3.2 Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements of MG-R (SVR) (including compliance with the Compliance Rules and SVR CP Specifications) in Licensed Products would pose a serious risk of rendering Licensed Products unable to receive, decrypt, or decode SVR Data. By way of example, a component that is soldered rather than socketed may be appropriate for this means.

3.4 Hybrid

The interfaces between Hardware and Software portions of a Licensed Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection which would be provided by a pure Software implementation.

3.5 Level of Protection

"Core Functions" of MG-R (SVR) include encryption, decryption, authentication, maintaining the confidentiality of Highly Confidential cryptographic algorithms and Device Key Set and preventing exposure of compressed, Decrypted SVR Data. The Core Functions of MG-R (SVR) shall be implemented in a reasonable method so that they:

3.5.1 Cannot be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips and soldering irons ("Widely Available Tools"), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debugging or decompilers ("Specialized Tools"), other than devices or technologies whether Hardware or Software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required by MG-R(SVR) ("Circumvention Devices"); and

3.5.2 Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section 3.5.1 such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

3.6 Delivery of Decrypted SVR Data to the functions described in Sections 3.1, 3.2, 3.3.1 (iii), 3.3.2 and 4.6 of Exhibit C shall be implemented in a reasonable method that is intended to make such functions difficult to defeat or circumvent by the use of Widely Available Tools, not including Circumvention Devices or Specialized Tools as defined in Section 3.5.1 of these Robustness Rules.

3.7 Advance of Technology

Although an implementation of a Licensed Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Licensed Product, would have caused such products to fail to comply with these Robustness Rules ("New Circumstances"). If Licensee has (a) actual notice of New Circumstances, or (b) actual knowledge of New Circumstances (the occurrence of (a) or (b) hereinafter referred to as "Notice"), then within eighteen (18) months after Notice such Licensee shall cease distribution of such Licensed Product and shall only distribute Licensed Products that are compliant with the Robustness Rules in view of the then-current circumstances.

Exhibit D-1
Robustness Checklist

Notice: This checklist is intended as an aid to the implementation of the Robustness Rules for hardware and software implementations of SVR CP Specifications in a Licensed Product. Licensor strongly recommends that you complete this Checklist for each Licensed Product before releasing any product and at a sufficiently early date in design, as well as during production, to avoid product compliance redesign delays. This Checklist does not address all aspects of SVR CP Specifications and Compliance Rules necessary to create a product that is fully compliant. Failure to perform necessary tests and analysis could result in a failure to comply fully with SVR CP Specifications, Compliance Rules or Robustness Rules in breach of the Agreement and, as a consequence, in appropriate legal action of Licensor and Eligible Content Participants.

Notwithstanding whether any particular design or production work is being outsourced or handled by contractors to the company, compliance with the above Rules remains the responsibility of this company.

Date:

Manufacturer:

Product Name:

Hardware Model or Software Version:

Name of Test Engineer Completing Checklist:

Test Engineer:

Company Name:

Company Address:

Phone Name:

Fax Number:

General Implementation Questions

1. Has the Licensed Product been designed and manufactured so there are no switches, buttons, jumpers, or software equivalents of the forgoing, or specific traces that can be cut, by which the content protection technologies, analog protection system, output restrictions, recording limitations, or other mandatory provisions of SVR CP Specifications or the Compliance Rules can be defeated or by which Decrypted SVR Data can be exposed to unauthorized copying?

2. Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can intercept the flow of Decrypted SVR Data or expose it to unauthorized copying?

3. Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the SVR CP Specifications or the Compliance Rules?

4. Does the Licensed Product have service menus, service functions, or service utilities that can alter or expose the flow Decrypted SVR Data within the device?

If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to expose or misdirect Decrypted SVR Data.

5. Does the Licensed Product have services menus, service functions, or service utilities that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of SVR CP Specifications or the Compliance Rules?

If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to defeat the content protection features of MG-R(SVR) (including compliance with the Compliance Rules and SVR CP Specifications).

6. Does the Licensed Product have any user-accessible buses (as defined in Section 2.1 of the Robustness Rules)?

If so, is Decrypted SVR Data carried on this bus?

If so, then:
Identify and describe the bus, and whether the Decrypted SVR Data is compressed or uncompressed. If such Data is compressed, then explain in detail how and by what means the data is being protected as required by Section 2.2 of the Robustness Rules.

7. Explain in detail how the Licensed Product protects the confidentiality of all keys.

8. Explain in detail how the Licensed Product protects the confidentiality of the confidential cryptographic algorithms used in MG-R(SVR).

9. If the Licensed Product delivers Decrypted SVR Data from one part of the product to another, whether among software modules, integrated circuits or otherwise or a combination thereof, explain how the portions of the product that perform authentication and/or decryption and the MPEG (or similar) decoder have been designed, associated and integrated with each other so that Decrypted SVR Data are secure from interception and copying as required in Section 3.1 of the Robustness Rules.

10. Are any MG-R (SVR) functions implemented in Hardware?
If Yes, compete hardware implementation questions.

11. Are any MG-R (SVR) functions implemented in Software?
If Yes, complete software implementation questions.

SOFTWARE IMPLEMENTATION QUESTIONS

12. In the Licensed Products, describe the method by which all Device Keys and Sets of Device Keys are stored in a protected manner.

13. Using the grep utility or equivalent, are you unable to discover any Device Key Set in bring images of any persistent memory devices?

14. In the Licensed Products, describe the method used to obfuscate the confidential cryptographic algorithms and Device Key Set used in MG-R (SVR) and implemented in software.

15. Describe the method in the Licensed Products by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Licensed Product) are created and held in a protected manner.

16. Describe the method being used to prevent commonly available debugging or decompiling tools (e.g., Softice) from being used to single-step, decompile, or examine the operation of the MG-R (SVR) functions implemented in software.

17. Describe the method by which the Licensed Products self-checks the integrity of component parts in such manner that modifications will cause failure of authorization or decryption as described in Section 3.2.2 of the Robustness Rules. Describe what happens when integrity is violated.

18. To assure that integrity self-checking is being performed, perform a test to assure that the executable will fail to work once a binary editor is used to modify a random byte of the executable image containing MG-R (SVR) functions, and describe the method and results of the test.

Hardware Implementation Questions

19. In the Licensed Product, describe the method by which all Device Key Set are stored in a protected manner and how their confidentiality is maintained.

20. Using the grep utility or equivalent, are you unable to discover any Device Key Set in binary images of any persistent memory devices?

21. In the Licensed Product, describe how the confidential cryptographic algorithms and Device Key Set used in MG-R (SVR) have been implemented so that they cannot be read.

22. Describe the method in the Licensed Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Licensed Product) are created and held in a protected manner.

23. Describe the means used to prevent attempts to replace, remove, or alter hardware elements or modules used to implement MG-R(SVR) functions.

24. In the Licensed Product, does the removal or replacement of hardware elements or modules that would compromise the content protection features of MG-R(SVR) (including the Compliance Rules, SVR CP Specifications, and the Robustness Rules) damage the Licensed Product so as to render the Licensed Product unable to receive, decrypt, or decode SVR Data?

Notice: This checklist does not supersede or supplement SVR CP Specifications, Compliance Rules, or Robustness Rules. The Company and its Test Engineer are advised that are elements of SVR CP Specifications and Compliance Rules that are not reflected here but that must be complied with.

SIGNATURES:

Signature of Test Engineer with Personal knowledge of Answers Date

Printed Name of Test Engineer with Personal Knowledge of Answers

EXHIBIT E-1
CONFIDENTIALITY AGREEMENT
ACKNOWLEDGMENT BY AUTHORIZED EMPLOYEES

To: ***(Company Name of Licensee or Licensee's Subsidiary)***

I, ***(Person's Name)***, a full-time employee of ***(Company Name of Licensee or Licensee's Subsidiary)*** (hereinafter referred to as "Licensee"), acknowledge that I have been designated by Licensee as an "Authorized Employee" (defined in the Memory Stick PRO - Secure Video Recording Format - Content Protection License Agreement between Sony Corporation and ***(Company Name of Licensee)*** made on ***(Month)*** ***(Date)***, ***(Year)*** (hereinafter referred to as the "Agreement")).

I acknowledge that I shall keep in confidence the Highly Confidential Information (as defined in the Agreement) of Sony Corporation designated as such by Sony Corporation to Licensee in accordance with the instructions given from time to time by Licensee during the period commencing on the signature date hereof and ending ten (10) years after the last date of manufacture by any entity of any product implementing MG-R(SVR) (as defined in the Agreement).

I further acknowledge that in the event I fail to abide by the terms as described above, Sony Corporation shall, in its sole discretion, be entitled to bring an action at law or in equity against ***(Company Name of Licensee or Licensee's Subsidiary)*** to claim damages.

By signing below, I attest that I have read and understood this acknowledgment and the Agreement.

Signed : ______________________

Name : ______________________

Title : ______________________

Date : ______________________

cc : Memory Stick Business Center
Micro Systems & Network Company
Sony Corporation

EXHIBIT E-2
ACKNOWLEDGMENT BY LICENSEE CONTACT

To: ***(Company Name of Licensee or Licensee's Subsidiary)***

I, ***(Name of the person)***, a full-time officer or employee of ***(Company Name of Licensee or Licensee's Subsidiary)*** (hereinafter referred to as "Licensee"), acknowledge that I have been designated by Licensee as a "Licensee Contact" (defined in the Memory Stick PRO - Secure Video Recording Format - Content Protection License Agreement made as of ***(Month) (Date), (Year)*** between Sony Corporation (hereinafter referred to as "Sony" and Licensee (hereinafter referred to as the "Agreement"), to receive "Highly Confidential Information" (as defined in the Agreement) on behalf of Licensee. I have also been designated by Licensee as an "Authorized Employee" (as defined in the Agreement) and have executed the "ACKNOWLEDGMENT BY AUTHORIZED EMPLOYEES" attached to the Agreement. In addition to the confidentiality obligations relating to Highly Confidential Information under the "ACKNOWLEDGMENT BY AUTHORIZED EMPLOYEES", as Licensee Contact, I further undertake as follows:

1. I shall receive Highly Confidential Information in the manner designated by Sony, and shall distribute such Highly Confidential Information only to necessary Authorized Employees of Licensee in accordance with ARTICLE IX of the Agreement.

2. Upon receipt from Sony of any revision to Highly Confidential Information, I shall distribute such revised Highly Confidential Information only to necessary Authorized Employees in accordance with ARTICLE IX of the Agreement.

3. Upon downloading any electronic version of Highly Confidential Information from the website designated by Sony in accordance with Sony' instructions, I shall immediately make the necessary and permitted number of hard copies of such Highly Confidential Information directly from such electronic version and distribute them only to the Authorized Employees of Licensee, and immediately delete such electronic version from all hard discs, servers and any other data storage instruments after making such hard copies.

4. The obligations set forth above shall be in full force until I am discharged from my role as Licensee Contact by Licensee provided that such discharge from my role as Licensee Contact shall not affect my confidentiality obligations under the Agreement